UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	
	:	
vs.	:	No. 4:04-CR-270
	:	
WILLIAM HEISER	:	(Judge Muir)

OPINION

MUIR, District Judge.

I. Introduction.

On August 12, 2004, a two-count Indictment was returned by a Grand Jury sitting in the Middle District of Pennsylvania charging William Heiser with sexual exploitation of children in violation of 18 U.S.C. § 2251(b) (Count 1) and knowingly receiving and distributing child pornography in violation of 18 U.S.C. § 2252A and § 2256(8)(B). The Government specifically alleges that Heiser "being the parent, legal guardian, and person having custody and control of a minor did unlawfully and knowingly permit such person to engage in sexually explicit conduct . . . for the purposes of producing visual depictions – digital images, computer images, and computer generated images – of such conduct . . ." and "unlawfully and knowingly receive[d] and distribute[d] material that . . . contain[ed] child pornography . . . ." The case is presently on our May, 2006, trial list for a non-jury trial.

On February 2, 2006, Heiser filed a motion entitled "Motion to Dismiss the Indictment or in the Alternative to

Suppress the Computer Evidence Due to Destruction of the Hard Drive." The matter was fully briefed and an evidentiary hearing was held on April 20, 2006. The following are the court's findings of fact, discussion and conclusions of law.

II. Findings of Fact.

1. On May 18, 2004, Berwick Police Officers seized one Discount Computer, 19 floppy disks and two zip 100 MB disks from Heiser's residence at 602 Green Street, Berwick, Pennsylvania. (Undisputed, hereinafter referred to as "U")

2. On September 16, 2004, the Government provided Heiser with a packet of discovery. (U)

3. Included in the discovery provided by the Government on September 16, 2004, was a one-page "General Investigation Report" dated June 28, 2004, prepared by Computer Crime Analyst Dale R. Young of the Bureau of Criminal Investigations Area II Computer Crime Task Force, Pennsylvania State Police. (U)

4. After receiving Defendant's computer on June 14, 2004, Mr. Young attempted to acquire an image (bit-by-bit identical copy) of Defendant's hard drive using standard and widely recognized forensic procedures but could only do so after several attempts because the computer and hard drive were in poor condition. (U)

5. Young observed that the cooling fan was inoperable,

causing the hard drive to overheat, and that the computer itself was covered in (sic) pet hair. (U)

6. Mr. Young states the following in his General Investigation Report dated June 28, 2004:

6.1 that he "conducted a forensic examination" of the computer seized from Heiser's residence; (U)

6.2 that "the hard drive image was acquired using EnCase software, and the F.R.E.D. (Forensic Recovery of Evidence Device) system which write protects the hard drive being acquired which does not allow any changes to be made to the hard drive"; (U)

6.3 that "[t]he image files were subsequently saved to the evidence drive of the F.R.E.D. and were viewed with EnCase"; (U)

6.4 that while searching HTML files found in unallocated space, "one file indicated 'Belarc Advisor,' a program for catalogueing (sic) an operating system and all the programs on a computer was run on Friday, April 30th, 2004, by Bill HEISER."; (U)

6.4.1 that with respect to the file regarding the Belarc Advisor, "[t]his document, which is attached to this report, shows all the software programs, users and registry settings installed on the computer being tested"; (U)

6.4.2 that Belarc Advisor “report showed that there were three users: Bill, Melissa, and Willie Heiser”; (U)

6.4.3 that according to the Belarc Advisor report “Jamie Heiser was not listed as a user on the computer”; (U)

6.5 that when he previewed the floppy disks and zip disks he found a disk labeled “2 of 6" which contained “eight files, apparently a diary written by” Jamie Heiser; (U)

6.6 that he “found 21 images of suspected child pornography in allocated space under the directory C:\program files\agent, and 495 images of suspected child pornography in unallocated space, some of which appear to be the suspect’s daughter Jaime HEISER”; (U)

6.7 that “[a]ll suspected child pornography images were copied to a CD and supplied to SGT. McCORMICK”; (U)

6.8 that “[n]o changes were made to the original hard drive at any time during the course of the examination”; (U)

6.9 that “[a]ll evidence was returned to Sgt. MCCORMICK on 8/11/04"; and

6.10 that an EnCase report is attached. (U)

6.10.1 The EnCase report was not attached to Mr. Young's General Investigation Report dated June 28, 2004, which was provided to defense counsel in discovery on September 16, 2004. (U)

6.10.2 By letter of December 13, 2005, the Government provided to defense counsel a 13-page EnCase Report. (U)

6.11 The Belarc Advisor document was not attached to Mr. Young's General Investigation Report dated June 28, 2004, received in discovery on September 16, 2004.

6.12 A Belarc Advisor document was provided to defense counsel by the Government on December 21, 2004. (U)

6.13 Heiser ultimately received in discovery what purports to be a copy of the 495 images of suspected child pornography in unallocated space copied to a CD on June 28, 2004, and supplied to Sgt. McCormick; (U)

6.14 Heiser has never received copies of the 21 images of suspected child pornography found in allocated space purportedly copied on June 28, 2004, to a CD and supplied to Sgt. McCormick.

6.15. Counsel for Heiser was permitted to view the 21 images of suspected child pornography found in allocated space.

6.16. The 21 images of suspected child pornography found in allocated space are not part of the present Indictment.

7. Mr. Young does not report in his General Investigation Report dated June 28, 2004, that he had difficulty getting the hard drive to be recognized by his forensic tower or that he discovered that the hard drive was not spinning. (U)

8. In June of 2004, Mr. Young obtained a bit-by-bit image copy of Mr. Heiser's hard drive.

9. The copy was stored on Mr. Young's computer hard drive, the evidence drive of the Forensic Recovery of Evidence Device.

10. EnCase prepared a report in connection with the investigation in this case which was approximately 100 pages. (U)

11. The Government has never provided the 100-page report to Heiser. (U)

12. The Berwick Police Department has lost the 100-page report. (U)

13. On November 1, 2004, Heiser filed a motion to compel discovery, seeking a mirror image of the computer hard drive along with copies of any software including disks which were seized from his residence on or about May 18, 2004. (U)

14. This court granted Heiser's discovery motion on December 16, 2004, and directed the parties to file a stipulated protective order within 20 days if the parties could agree upon

the form. (U)

15. In December 2004, Mr. Young's computer hard drive, which contained the copy of the image from Defendant's hard drive and files from approximately 15 other cases that Mr. Young was working on suffered a catastrophic failure. (U)

16. "Mean Time to Failure" is a standard used in the computer industry to measure the reliability of hardware such as hard drives. (U)

17. Mr. Young's hard drive was less than two years old and well within the "Mean Time to Failure" rating for the drive, so he had no reason to expect the drive to fail without warning.

18. Upon the failure of Mr. Young's hard drive, Mr. Young in April 2005 tried to obtain another bit-by-bit copy from Heiser's hard drive.

19. Because of the poor condition of Defendant's hard drive, it also failed, and multiple attempts to make an image copy were unsuccessful. (U)

20. Mr. Young observed so many errors in the attempted re-imaging of Defendant's hard drive that he is of the opinion that the platters, or parts of the drive containing the magnetic material used to store the data, were damaged. (U)

21. Defendant's hard drive is no longer readable, and the Government has been unsuccessful in making another image copy

of it. (U)

22. In Mr. Young's opinion, the hard drive has been physically damaged and cannot be made functional so that the data on it may be read and imaged. (U)

23. It is the standard practice of the Pennsylvania State Police to make an identical image copy of a computer hard drive from the original and to conduct tests solely on the image copy in order to maintain the integrity of the original evidence.

24. In the event that there is a failure of the image copy of a hard drive, it is the practice of the Pennsylvania State Police to re-image or make another bit-by-bit copy of the hard drive from the original evidence.

25. Mr. Young followed all Pennsylvania State Police evidence protocols and procedures in this case.

26. Mr. Young also made a bit-by-bit CD-ROM backup copy of Defendant's hard drive and provided that copy to the Berwick Police Department.

27. Mr Young was aware of this Court's order of January 7, 2005, a few days after it was signed which required the Government to provide Heiser with a bit-by-bit image copy of the hard drive.

28. Mr. Young intially believed that there was no need to re-image Defendant's hard drive after the evidence computer, F.R.E.D. hard drive, failed since the Berwick Police Department

had previously been provided a copy.

29. Despite requests from Mr. Young, the Berwick Police Department has been unable to produce the backup copy, as well as the 100-page EnCase report generated in this case.

30. When Mr. Young realized that the Berwick Police Department backup copy was missing, he requested that the department return the original evidence to him, including Defendant's hard drive, so that he could attempt to make another image copy.

31. The Berwick Police Department lost its bit-by-bit image copy of Defendant's hard drive.

32. A stipulated protective order was filed on January 7, 2005, pursuant to which the Government agreed to provide and was directed to provide defense counsel with a bit-by-bit image copy of the computer hard drive and copies of all disks and zip disks seized from Defendant's residence. (U)

33. On or about June 9, 2005, the Government provided Heiser with CD-ROMs copied from Heiser's computer. (U)

34. The Government has never provided to Heiser's counsel a bit-by-bit image of the computer hard drive or copies of all disks and zip disks seized from Heiser's residence. (U)

35. On or about July 1, 2005, Mr. Young informed case agent, FBI Special Agent James Kyle, through a letter, that Defendant's original hard drive and Young's evidence drive on

which he had stored an image copy of Defendant's drive had both suffered catastrophic failures. (U)

36. On July 15, 2005, defense counsel sent a letter to Assistant United States Attorney Chris Fisanick requesting (1) the computer evidence set forth in the Stipulated Protective Order filed January 7, 2005, (2) the Computer Analysis Response Team (CART) reports and (3) the 100-page report prepared by Dale Young. (U)

37. During the time between this Court's order (January 7, 2005) and the letter (July 1, 2005) formally advising Special Agent Kyle that it would be impossible to image Defendant's hard drive because of two catastrophic failures, Mr. Young was working on other cases, and the Defendant's hard drive was in the custody of the Berwick Police Department for use in a state court jury trial for part of that time.

38. On August 2, 2005, Heiser filed a second motion to compel discovery and a brief in support thereof, seeking the Government's compliance with the Stipulated Protective Order of January 7, 2005, a bit-by-bit image of the computer hard drive along with copies of all disks and zip disks seized from Heiser's residence and the reports of computer analysis. (U)

39. On August 2, 2005, by facsimile, the Government provided defense counsel with a copy of a letter dated July 1, 2005, from Dale Young to Special Agent Kyle, which set forth his

assessment of the conditions of the hard drive removed from the computer seized from Mr. Heiser's residence. (U)

40. Mr. Young writes in his letter of July 1, 2005:

40.1 that "[u]pon our initial acquisition of the hard drive on 6/14/2005, I had difficulty getting the hard drive to be recognized by our forensic tower, and discovered the issue to be that the hard drive motor was not spinning"; (U)

40.2 that he "was able to get the hard drive to spin after several attempts using three different forensic devices, and was able to successfully acquire the hard drive image; (U)

40.3 that "[o]nce imaged, the hard drive was then replaced into the computer and the forensic exam was performed, the reports from which were printed and supplied to Berwick PD"; (U)

40.4 that "Mr. HEISER's computer was also returned to Berwick PD for further disposition."; (U)

40.5 that "[b]etween 06/14/2005 (sic) and Mr. HEISER's trial, the computer sat in evidence and was never powered up"; (U)

40.6 that "[i]n December of 2004, the evidence drive where I keep any cases I've worked on until final disposition of those cases suffered a catastrophic

failure and all of my files regarding Mr. HEISER were lost, along with approximately 15 other cases"; (U)

40.7 that "[w]hen Berwick PD informed me in April of 2005 that Mr. HEISER would have his trial soon, I requested that the computer be brought back to this lab for a re-acquisition for review"; (U)

40.8 that in April of 2005, "[w]hen the hard drive was removed from the computer and placed into the forensic machine, the same problem as originally reported had once again occurred. The drive motor would not spin"; (U)

40.9 that "it took several serious attempts to get the motor to spin again, but on acquisition there were so many errors, that it was apparent the platters in the hard drive were damaged" (U)

40.10 that in his opinion, "based on previous issues dealt with while acquiring the image from the hard drive, the hard drive was beginning to seize in June of 2004"; (U)

40.11 that "[h]aving been powered off for almost a year, the motor in the hard drive completely seized up to the point that when it was finally forced to spin it damaged the hard drive platters, making the drive no longer functional"; and (U)

40.12 that "[t]he hard drive, if the motor were to be replaced in a clean room, would still have errors due to the physical damage caused by the seized motor, and would in all likelihood not be readable even if it did spin up." (U)

41. Mr. Young's initial acquisition of the hard drive actually occurred on June 14, 2004, not June 14, 2005. (U)

42. Mr. Young did not report in his General Investigative report of June 28, 2004, that he experienced difficulty getting the hard drive to be recognized by the forensic tower or that the hard drive motor was not spinning. (U)

43. Mr. Young did not report the difficulty in acquiring the hard drive in his General Investigative Report dated June 28, 2004. (U)

44. Mr. Young did not set forth in his letter of July 1, 2005, what were the three forensic devices used to acquire the hard drive image. (U)

45. Mr. Young's letter of July 1, 2005 lists his credentials as follows: "MCSA, MCSE, CCNA, CFCE, CEECS, A+, Certified Steganography Examiner." (U)

46. MCSA is a Microsoft Certified Systems Administrator. (U)

47. MCSE is a Microsoft Certified Systems Engineer. (U)

48. CCNA is a CISCO Certified Network Associate. (U)

49. CFCE is a Certified Forensic Computer Examiner. (U)

50. CEECS is a Certified Electronic Evidence Collection Specialist. (U)

51. Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured. (U)

52. Standard operating procedures require backing up materials. (U)

53. According to Kevin H. Peden, Computer Forensic Analyst of Global CompuSearch LL, “every piece of electronic evidence should have a valid ‘back up’ copy.” (U)

54. According to Mr. Peden “[i]t is the standard operating procedure of Global CompuSearch LLC, always to create a secondary copy of evidentiary media when we are the collecting agency” and “[t]he first copy is stored in our evidence safe as a safeguard against the loss of evidence.”

55. According to Mr. Peden, as a former police officer, he recognizes ‘the importance of safeguarding evidence until it is turned over to the court system.” (U)

56. On August 26, 2005, the Government filed a Brief

in Opposition to the Second Motion to Compel Discovery and attached the letter from Dale Young dated July 1, 2005, as an exhibit. (U)

57. With respect to the bit-by-bit miror image of the computer hard drive, the Government represented that the computer hard drive has failed and is now "inoperable and unreadable, thereby rendering any atempt to make copies futile." (U)

58. With respect to the zip disks, the Government claimed that it was in the process of making forensic copies of the zip disks at CART headquarters in Philadelphia and would provide them as soon as possible. (U)

59. With respect to the 100-page report of Dale Young, the Government believed it had produced all of Mr. Young's material. (U)

60. The Government later produced a 13-page EnCase Report on December 13, 2005. (U)

61. The Government has never produced the 100-page report. (U)

62. The 100-page EnCase report was lost when Mr. Young's evidence computer failed in December 2004.

63. With respect to the CART reports , on August 4, 2005, the Government provided one CART Examination Report dated April 27, 2005, regarding a Zip 100 Disk labeled "Archive Disk 7." (U)

64. The Government has not provided any other CART reports. (U)

65. As part of the discovery process, defense counsel has been provided with copies of the computer evidence – though not a bit-by-bit image copy of the hard drive – that is in the possession of the FBI and Pennsylvania State Police. (U)

66. As part of the discovery process, defense counsel has, on several occasions, had the opportunity to inspect the Government's evidence in this case. (U)

67. Because of the failure of the two hard drives, and despite making a diligent search, the Government does not have an image copy of Defendant's hard drive in its possession and thus could not provide Defendant with a bit-by-bit image copy of the hard drive.

68. The hard drive contained evidence against Mr. Heiser. (U)

69. According to Mr. Young, the images of suspected child pornography were found on the hard drive. (U)

70. Without the computer hard drive, Heiser cannot determine the date and time that any particular file was deleted. (U)

71. According to Mr. Peden, "[i]f multiple people had access to the computer it is important to examine how many users had access to the computer and attempt to determine who was using

the computer at the time the incident(s) occurred." (U)

72. Without the computer hard drive, Heiser cannot determine when the items in question appeared on the computer. (U)

73. According to Mr. Peden "[a]lthough it is not always possible to establish this, many times we can establish a general time when the suspect material appeared on the computer."(U)

74. According to Mr. Peden "[w]hen the evidence resides in unallocated file space, (that area of the drive which houses the information that has been deleted and is available for new data to be written), it is still possible to determine, in some instances, when that information more than likely appeared on the computer." (U)

75. In approximately 200 forensic hard drive examinations, Mr. Young has never experienced two nearly simultaneous, catastrophic hard drive failures with the loss of original evidence as he did in this case. (U)

76. Mr. Peden has never experienced two nearly simultaneous catastrophic hard drive failures as happened in this case. (U)

77. A bit-by-bit image of the computer hard drive could potentially be helpful to Heiser.

78. Heiser cannot determine from the discovery data,

i.e., the computer evidence, delivered by the Government the date and time that any particular file was created.

79. Heiser cannot determine from the discovery data delivered by the Government the date and time any particular file was last accessed.

80. Heiser cannot determine from the discovery data delivered by the Government who had access to the computer during any of the crucial times.

81. The Government knew from its examination of the hard drive in June of 2004, that there were multiple users of that one computer in the Heiser household. (U)

82. Mr. Young testified at Mr. Heiser's Columbia County trial that Jamie Heiser also used the computer. (U)

83. Within the discovery provided by the Government, there are chats between certain individuals including "DJ-Gary1" or "Gary-dj1" who identifies himself as Gary Pursel of 220 West Main Street, Bloomsburg, Pennsylvania, and "rebecca91574" or "lollipoplick" who identifies herself as Rebecca Dawn Chason Hathaway of 2722 Needle Palm Drive, Edgewater, Florida. (U)

84. In April of 1999, during chats between Gary Pursel and Rebecca Hathaway, Gary tells Rebecca that he is at Bill's house. (U)

85. Within the discovery provided by the Government, there are chats between individuals with a variety of screen

names including “Zapata64.” (U)

86. The Government has not provided any evidence to show the identity of “Zapata64.”

87. Mr. Young testified that there is no way from a chat log to figure out who is doing the chatting. (U)

88. The computer hard drive is irreplaceable. (U)

89. Mr. Heiser is unable to obtain comparable evidence by other reasonably available means. (U)

90. The computer hard drive is potentially useful to the defense. (U)

91. If the hard drive had been produced in accordance with the Stipulated Protective Order of January 7, 2005, a defense expert may have been able to determine who had access to the computer. (U)

92. If the hard drive had been produced in accordance with the Stipulated Protective Order of January 7, 2005, a defense expert may have been able to determine who was using the computer at the time of the incident(s). (U)

93. If the hard drive had been produced in accordance with the Stipulated Protective Order of January 7, 2005, a defense expert may have been able to determine whether the evidence was altered in any way. (U)

94. If the hard drive had been produced in accordance with the Stipulated Protective Order of January 7, 2005, a

defense expert may have been able to determine the habits and/or interests of those using the computer. (U)

95. The Government did not report the unavailability of a bit-by-bit image of the computer hard drive to the defense until August 2005. (U)

96. Mr. Young testified that the evidence acquired on the second attempt to acquire the hard drive was not a bit-by-bit exact copy of the hard drive seized from Heiser's residence according to the hash values. (U)

97. Mr. Young testified that he copied an image of the hard drive onto CDs which were provided to Sgt. McCormick of the Berwick Police. (U)

98. Mr. Young testified that there is no chain of custody report showing his provision of the CDs to Sgt. McCormick of the Berwick Police. (U)

99. The General Investigation Report prepared by Dale Young on June 28, 2004, does not state that CDs were given to Sgt. McCormick of the Berwick Police. (U)

100. Mr. Young testified that at the time he initially imaged the hard drive seized from William Heiser's residence, the Pennsylvania State Police did not have a manual setting forth procedures for handling computer evidence. (U)

101. Mr. Young testified that the procedures under which he operated were verbally passed down to him by the Trooper

that trained him. (U)

102. Mr. Young testified that the integrity of the copy of the hard drive that he made during the second acquisition is low. (U)

103. Mr. Young testified that when he exported from EnCase, he did not export the index.dat files, the e-mail files, all documents, or all link files to a disk. (U)

104. Mr. Young testified that if he would have had a backup copy maintained in his evidence locker, he would not have lost all of this evidence. (U)

105. Mr. Young testified that the 13-page EnCase report does not reflect every single file found on the seized hard drive and does not reflect all the dates and times that accompany those files. (U)

106. Mr. Young testified on redirect that he has no paperwork indicating provision of copies of the evidence to the Berwick Police. (U)

107. Mr. Young testified on redirect that the CDs given to the Berwick Police were not original evidence.

108. Kevin Peden testified that a hash value is a digital fingerprint created by a mathematical calculation which derives a number. (U)

109. Kevin Peden testified that where a verification hash value is exactly the same as the hash value on the original

evidence, the evidence imaged is an exact replica. (U)

110. Kevin Peden testified that if the hash value on the evidence images is one number off, compared to the hash value of purportedly the same evidence, then they are not reliable copies. (U)

111. Mr. Young testified that he gave a copy of the evidence on CDs to the Berwick Police Department but he has no record of doing so. (U)

112. Mr. Young testified that he could not recall how many CDs were given to the Berwick Police Department. (U)

113. Mr. Young testified that the Berwick Police Department has since lost the CDs but there is no record of that either. (U)

114. Mr. Young did not advise FBI Agent Kyle either of the provision of the CDs to the Berwick Police Department or the ultimate loss of the CDs by the Berwick Police Department in his letter of July 1, 2005 (Defendant's Exhibit 6). (U)

115. Mr. Young's General Investigation Report date June 28, 2004, made no mention of the difficulties he had with the hard drive upon initial acquisition. (U)

116. Mr. Young could not recall if he had made notes concerning the difficulties he had with the computer upon initial acquisition. (U)

117. Evidence of a copy provided to and ultimately

lost by the Berwick Police Department was first disclosed at the evidentiary hearing on April 20, 2006. (U)

118. Defense counsel was not advised of the loss of evidence in December, 2004, or unsuccessful attempted reacquistion in April, 2005, until August 2, 2005. (U)

119. Mr. Young does not recall if he took any notes or made any report concerning that "catastrophic failure" of the evidence hard drive. (U)

120. Mr. Young's General Investigation Report (Exhibit D-2) is dated June 28, 2004. (U)

121. The last sentence of the Recommendations/Comments section of the General Investigation Report states that "[a]ll evidence was returned to Sgt. MCCORMICK on 8/11/04." (U)

122. The reference to the return of evidence on 8/11/04 and the report dated 6/28/04 shows that Mr. Young amended his report. (U)

123. Mr. Young did not write a separate report supplementing his report of 6/28/04 concerning the return of evidence. (U)

124. The defense learned for the first time at the hearing on April 20, 2006, that the Berwick Police Department was given CDs containing an image of the hard drive in the computer taken from Heiser's residence. (U)

125. Mr. Young testified that he has no record of

provision of evidence taken from the computer to Special Agent James Kyle. (U)

126. When Mr. Young first tried to make an image of the hard drive in the computer taken from Heiser's residence, he had great difficulty. (U)

127. Initially, Mr. Young could not get the hard drive to spin. (U)

128. The cooling fan of the computer was not working which caused it to overheat. (U)

129. The computer was dirty and covered in pet hair. (U)

130. The computer taken from Heiser's residence sat in evidence and was not powered up for at least ten (10) months, from June, 2004, to sometime after April, 2005. (U)

131. Mr. Young testified that damage can be caused simply when a hard drive sits and is not powered up, especially one which is "in as bad shape" as the one in this case. (U)

132. Although the FBI knew of the loss/destruction of evidence in January, 2005, the defense was not informed until August, 2005. (U)

III. Discussion.

Heiser contends that the Government destroyed critical evidence in this case, the computer hard drive, and that he is therefor entitled to dismissal of the Indictment or suppression

of the evidence, the pornographic images. Both the Government and Heiser refer to two United States Supreme Court cases dealing with the destruction of evidence by the Government.

The first case referred to by both counsel deals with a policy of the State of California to discard breath samples obtained from those suspected of driving under the influence of alcohol. California v. Trombetta, 467 U.S. 479, 104 S.Ct. 2528 (1984). In Trombetta there was a set policy and procedure to destroy the evidence. The evidence was intentionally destroyed per the policy. The Supreme Court reviewed the policy and determined that it did not violate the defendant's due process rights.

The second case referred to by both counsel deals with the failure of the police to preserve properly semen samples. Arizona v. Youngblood, 488 U.S. 51 (1988). In Youngblood, a ten-year-old boy was molested by a middle-aged man. After the assault the boy was taken to the hospital where a physician collected semen from the boy's rectum. The police also collected the boy's clothing which they failed to refrigerate. Tests were subsequently conducted on the rectal swabs and the boy's clothing but no useful information was obtained. A defense expert testified that Defendant may have been completely exonerated by timely performance of tests on properly preserved semen samples. The Supreme Court held that the Due Process Clause of the

Fourteenth Amendment did not require the State to preserve the semen samples even though the samples might have been useful. The Court held that "unless a criminal defendant can show bad faith on the part of the police, failure to preserve potentially useful evidence does not constitute a denial of due process of law." Id. at 58

In this case there was no intentional destruction of evidence. Furthermore, although the hard drive had possible exculpatory value, there was no apparent exculpatory value at the time it failed. The hard drive had both potential exculpatory and inculpatory value at the time it was seized by the police and at the time it failed. Under the facts of this case as set forth in Part II of this opinion, in order to establish a due process violation Heiser must demonstrate that the Government acted in bad faith. Youngblood, supra.

Heiser argues that Mr. Young engaged in bad faith when he failed to make and retain a back-up bit-by-bit image copy of the hard drive. Heiser further argues that under the circumstances of this case the failure to make a back-up copy was reckless. As set forth in Part II of this opinion, although Mr. Young did not retain an extra or backup copy, Mr. Young did make a bit-by-bit copy of the hard drive and provided that copy to the Berwick Police Department. Mr. Young may have been negligent when he failed to make and retain a back-up copy. However, we

cannot conclude that he acted in bad faith. "Bad faith" requires more than negligence or recklessness. Youngblood, at 58 ("In this case, the police collected the rectal swab and clothing on the night of the crime; respondent was not taken into custody until six weeks later. The failure of the police to refrigerate the clothing and to perform tests on the semen samples can at worst be described as negligent.").

The failure to make a back-up copy in our case is similar to the failure of the police to refrigerate and test evidence found by the Supreme Court in Youngblood to be at most negligent conduct. In our case the Government made a bit-by-bit working copy of the hard drive and also made a copy which was provided to the Berwick Police Department. Three events occurred which resulted in the loss of the evidence in our case: Mr. Young's computer failed, the re-imaging of Heiser's hard drive was unsuccessful and the Berwick Police Department lost its copy. "Bad faith" with respect to destruction of evidence requires more than mere negligence, it requires ill-will towards Heiser or a conscious effort to frustrate his defense. None of the events which resulted in the loss of the evidence in this case were intentionally caused by or resulted from bad faith of the Government.

IV. Conclusions of Law.

1. Defendant Heiser has failed to prove by a

preponderance of the evidence that the Government acted in bad faith by failing to preserve Heiser's computer hard drive.

2. The Government did not act in bad faith at any time in this case.

3. Defendant's proposed remedies of either suppression of the computer evidence or dismissal of the Indictment are inappropriate under the circumstances of this case.

3. Despite the lack of a bit-by-bit image of Defendant's hard drive, Defendant has the necessary discovery in his possession in order to prepare a defense.

An appropriate order will be entered.

s/Malcolm Muir
MUIR, U.S. District Judge

Dated: April 28, 2006

M:gs

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	
	:	
vs.	:	No. 4:04-CR-270
	:	
WILLIAM HEISER	:	(Judge Muir)

ORDER

April 28, 2006

Defendant's motion entitled "Motion to Dismiss the Indictment or in the Alternative to Suppress the Computer Evidence Due to Destruction of the Hard Drive" (Doc. 74) is denied.

s/Malcolm Muir
MUIR, U.S. District Judge

M:gs